Before the
Federal Communications Commission

In the Matter of	)	
	)	
Communications Assistance for	)	RM-10865
Law Enforcement Act Joint Petition	)	
For Rulemaking	)	
	)	

COMMENTS OF
THE ELECTRONIC PRIVACY INFORMATION CENTER

Introduction

Pursuant to the Commission's public notice[1] seeking comment on a Joint Petition for Expedited Rulemaking[2] concerning the Communications Assistance for Law Enforcement Act ("CALEA") filed by the Department of Justice, the Federal Bureau of Investigation, and the Drug Enforcement Administration (collectively "DOJ"), the Electronic Privacy Information Center ("EPIC") submits these comments. EPIC opposes the DOJ petition on the ground that it impermissibly seeks to extend the narrow, legislatively authorized reach of CALEA requirements from telecommunications providers to Voice over IP ("VoIP") services and broadband Internet Service Providers ("ISPs"). Any such expansion of CALEA's reach, should it be deemed necessary, must be effectuated by Congress — not the Commission — particularly in light of the unique privacy issues that arise when surveillance capabilities are mandated for packet-mode communications. Further, DOJ has not demonstrated that the existing CALEA regime is in any way inadequate to address its needs.

EPIC has been involved in many of the emerging privacy issues addressed by the Commission, including Caller ID, the TCPA, CPNI, location privacy, and most recently the adoption of the Do Not Call regulations. In particular, EPIC has been closely involved with

[1] Comments Sought on CALEA Petition Rulemaking, RM-10865 (Mar. 12, 2004).

[2] Joint Petition for Expedited Rulemaking, *In the Matter of Joint Petition for Rulemaking to Resolve Various Outstanding Issues Concerning the Implementation of the Communications Assistance for Law Enforcement Act*, RM-10865 (Mar. 10, 2004) ("Joint Petition").

CALEA since its controversial enactment in 1994.[3] EPIC has advocated for privacy protection in previous CALEA proceedings before the Commission, and addressed the privacy implications of the CALEA requirements before the Court of Appeals for the D.C. Circuit.[4] Last December, EPIC urged the Commission to adopt strong privacy protections in VoIP, and discussed its concern that extending CALEA to VoIP would establish unprecedented regulation for new communications services.[5]

In response to the Joint Petition, the Commission should recognize, consistent with Congressional intent and previous Commission statements, the narrow statutory reach of CALEA and the problematic issues that would arise if CALEA's requirements were extended to packet-mode services such as Internet Protocol ("IP")-based networks and VoIP services. The Commission should also recognize that Congress has established specific procedural requirements to protect against the unauthorized surveillance and/or interception of communications, and any modification or expansion of those legislative requirements must be made by Congress, not the Commission. In light of the clear, unambiguous statutory exclusion of information services such as ISPs, the difficult legal and technical problems of distinguishing content from call-identifying information, and the potential for unauthorized collection of third-party data, only Congress may consider extending the reach of CALEA to cover VoIP and other Internet services. Absent such Congressional action, the Commission should not accept DOJ's invitation to tread where Congress has not yet gone.

I. Congress Expressly Limited The Reach Of CALEA

Extending CALEA requirements to VoIP and ISPs, as DOJ urges, would contradict the plain language of CALEA, ignore the legislative intent behind the statute, and upset the delicate balance between privacy protection and law enforcement access. Extending CALEA in the manner proposed by DOJ would require legislative revision of CALEA and is beyond the Commission's statutory authority. When it drafted CALEA, Congress sought to strike a careful balance that protects the privacy rights of citizens while enabling legitimate law enforcement

[3] EPIC Statement on the Passage of CALEA (October 1994) *at* http://www.epic.org/privacy/wiretap/calea/epic_calea_statement.html.

[4] *United States Telecom Association v. Federal Communications Commission*, 227 F.3d 450 (D.C. Cir. 2000).

[5] Letter from EPIC, to the Federal Communications Commission (December 9, 2003) *available at* http://www.epic.org/privacy/voip/fccltr12.15.03.html.

access where authorized. Congress thus restricted CALEA compliance only to those telecommunications systems where law enforcement has traditionally had access, and establishing mandated procedures to protect the privacy of communications. Congress specifically found that broad application of CALEA to *all* electronic communications services was "neither practical nor justified to meet any law enforcement need."[6] Such a broad approach is precisely what DOJ now seeks.

Congress was clearly concerned about the implications of imposing CALEA requirements on information services such as the Internet and those commonly found on IP-based networks. The language of CALEA thus unambiguously excludes information services such as e-mail and Internet access.[7] The legislative history of CALEA unequivocally states that "[t]he only entities required to comply with the functional requirements are telecommunications common carriers, the components of the public-switched network where law enforcement agencies have always served most of their surveillance orders."[8] The legislative history is equally clear that "excluded from [CALEA's] coverage are "*all* information services, such as Internet service providers or services such as Prodigy and America-On-Line."[9] The narrow scope of CALEA's mandate is best summarized by the legislative history's explanation that "the bill does not require reengineering of the Internet, nor does it impose prospectively functional requirements on the Internet . . . ."[10]

Indeed, the Commission's previous interpretations of CALEA have reflected this careful legislative balance and recognized the limited scope of its mandate. The Commission has long recognized that CALEA expressly excludes "information services" from assistance capability requirements.[11] Further, the Commission has recognized that CALEA applies to packet data and

---

[6] H.R. REP. NO. 103-827, pt. 1 at 18 (1994).

[7] CALEA § 103(b)(2)(A). *See also United States Telecom Assoc., et al. v. Federal Communications Commission*, 227 F.3d 450, 455 (D.C. Cir. 2000) ("CALEA does not cover 'information services' such as e-mail and internet access.") (citing 47 U.S.C. §§ 1001(8)(C)(i), 1002(b)(2)(A)).

[8] H.R. REP. NO. 103-827, pt. 1 at 18 (1994).

[9] *Id.* at 18 (emphasis added).

[10] *Id.* at 23.

[11] Further Notice of Proposed Rulemaking, *In Re Communications Assistance for Law Enforcement Act*, CC Docket No.97-213, FCC 98-282 (rel. Nov. 5, 1998) (hereinafter "FNPRM").

packet-mode services only "to the extent [packet data] is used to provide telecommunications services, *and not for information services.*"[12]

In light of the clear Congressional intent that information services be excluded from the CALEA requirements, an extension of surveillance requirements to such networks could only occur if Congress revisited CALEA and addressed DOJ's stated concerns. It is not for the Commission to extend the statutory mandate to networks and technologies that Congress clearly sought to exclude.

II. Expansion of CALEA'S Coverage Would Raise Complex and Novel Issues That Should Be Addressed By Congress, Not the Commission

Applying CALEA's requirements to VoIP and high speed ISPs, as DOJ proposes, would raise difficult and unique privacy issues that arise when surveillance capabilities are mandated for packet-mode communications. If the Commission extended the reach of CALEA to technological environments that Congress did not anticipate in 1994 (and thus did not address), surveillance mandates would be imposed without the corresponding privacy protections unique to the packet-mode realm. Because, as the D.C. Circuit has held, CALEA does not authorize the Commission "to modify . . . [the] procedural safeguards for securing legal authorization to obtain" packet-mode communications,[13] the Commission would be unable to mandate appropriate procedures to address the unique privacy challenges that arise in the context of the Internet and related technologies. Those challenges fall into two categories: the addressing/content distinction, and potential unauthorized collection of third-party data. We address them in turn.

A. The Addressing/Content Distinction

The privacy issues that arise when law enforcement executes a pen register or trap and trace order in a packet-mode environment are familiar to the Commission, which has noted that "privacy concerns could be implicated if carriers were to give to [law enforcement] packets containing both call-identifying and call content information when only the former was

[12] *Third Report and Order, Communications Assistance for Law Enforcement Act*, CC Docket No. 97-213, FCC 99-230 (August 31, 1999) ("Third Report"), ¶48 (emphasis added).

[13] *United States Telecom Assoc., et al. v. Federal Communications Commission*, 227 F.3d 450, 465 (D.C. Cir. 2000).

authorized."[14] Congress also appears to have been cognizant of the issue when it enacted CALEA; it included in the statute an amendment to the pen register statute to require law enforcement, when executing a pen register, to use equipment "that restricts the recording or decoding of electronic or other impulses to the dialing and signaling information utilized in call processing."[15] Likewise, when Congress included a provision in the USA PATRIOT Act extending pen register authority to collect "dialing, routing, addressing, or signaling information," it specified that "such information shall not include the contents of any communication."[16]

Despite this recognition that pen register authority implicates the potential unauthorized capture of the "content" of communications when packet data is the object of surveillance, there is no clarity on the question of what constitutes "content." The Justice Department, in "field guidance" discussing the PATRIOT Act amendment, conveys a narrow interpretation of the "content" restriction: "Pen/trap orders cannot . . . authorize the interception of the content of a communication, such as words in the 'subject line' or the body of an e-mail."[17] The guidance is silent on other obvious "content" issues, such as the status of URLs captured during surveillance of "Web surfing" activity. While the URL "http://www.google.com" might be the functional equivalent of a telephone number, and thus characterized as "call-identifying" information in CALEA parlance, the URL "http://www.google.com/search?hl=en&lr=&ie=UTF-8&oe=UTF-8&q=Iraq+war+protest&btnG=Search" — generated during the course of an online search — clearly contains "content." Yet the Justice Department has not publicly addressed the status of URLs, nor proposed any technological means of parsing "call-identifying" information from "content" when monitoring online activity under pen register authority.

The unresolved questions surrounding the capture of URLs are illustrative of the issues that arise when surveillance requirements are imposed upon new communications technologies. EPIC submits that the resolution of such issues are best left to Congress, and that the expansion

---

[14] Third Report, ¶ 48.

[15] CALEA § 207(b), codified at 18 U.S.C. § 3121(c).

[16] USA PATRIOT Act, Pub. L. No. 107-56, § 216(c), *codified at* 18 U.S.C. § 3127(3).

[17] Department of Justice, *Field Guidance on New Authorities That Relate to Computer Crime and Electronic Evidence Enacted in the USA Patriot Act of 2001*, available at http://www.usdoj.gov/criminal/cybercrime/PatriotAct.htm.

of CALEA coverage proposed by DOJ, if adopted by Congress, would likely be balanced by concomitant privacy safeguards of the sort that the Commission is not empowered to impose.[18]

B. Unauthorized Collection of Third-Party Data

While the Commission has recognized the privacy issues that arise from the legal distinction between addressing information and communications content, it has not had occasion to consider a second, perhaps more problematic, by-product of surveillance of packet-data networks. Since the Commission issued its Third Report in 1999, it has become apparent that law enforcement access to network traffic can result in the interception of communications of third parties not named or identified in court surveillance orders — a phenomenon that never occurred in the traditional, circuit-switched telephone environment. As such, the expansion of CALEA's technical requirements urged by DOJ would make it difficult, if not impossible, for carriers to comply with the statutory command that they protect "the privacy and security of communications and call-identifying information not authorized to be intercepted." [19]

Internal FBI documents obtained by EPIC through Freedom of Information Act litigation show, beyond question, that surveillance conducted in packet-mode environments can result — and indeed *has* resulted — in the unauthorized capture of third-party communications. In a declaration submitted to the U.S. District Court for the Central District of California in January, 2000, an FBI Special Agent described the operation of the Bureau's packet-mode surveillance device, Carnivore:

> Although *the program is capable of capturing more than the information authorized* under the [court] order, I or the installing technicians will configure the program in a manner that will prevent the program from capturing any information that is not authorized under the order.[20]

---

[18] For example, when Congress extended the reach of pen register authority in the USA PATRIOT Act, it also imposed a new reporting requirement on law enforcement when it " install[s] and us[es] its own pen register or trap and trace device on a packet-switched data network of a provider of electronic communication service to the public." The provision requires strict documentation of the configuration of the surveillance device, specific times of use, and the identification of all data captured. USA PATRIOT Act, Pub. L. No. 107-56, § 216(b)(1), *codified at* 18 U.S.C. § 3123(a).

[19] CALEA § 103(a)(4), *codified at* 47 U.S.C. § 1002(a)(4).

[20] Declaration executed by Edward Hill, dated January 31, 2000 (attached hereto as Exhibit A); *also available at* http://www.epic.org/privacy/carnivore/fbi_dec.html (emphasis added).

The agent left no doubt that the potential unauthorized collection, if it occurred, would involve the communications of ISP customers not named in the court order:

> [T]he computer used to run the [Carnivore] program has limited memory capacity and limited ability to process information. Because of these limitations the computer used to run the program would be overloaded within a few minutes if it attempted to collect all of the information on Earthlink's 8 to 10 million e-mail messages.[21]

The precautions described in the declaration apparently are not always effective. An internal FBI document shows that, little more than a month later, Carnivore surveillance performed by the Bureau's "UBL [Usama bin Laden] Unit" resulted in the unauthorized acquisition of "E-Mails on non-covered" individuals — a clear violation of federal wiretap law. The overcollection occurred after the Carnivore "software was turned on and did not work correctly." According to the Bureau document, the "FBI technical person was apparently so upset that he destroyed all the E-Mail take, including the take on [the authorized target]." The report, dated April 5, 2000, and sent to M.E. (Spike) Bowman, Associate General Counsel for National Security Affairs, describes the incident as part of a "pattern" indicating "an inability on the part of the FBI to manage" its electronic surveillance activities.[22]

Two Bureau memoranda written one week later further document Carnivore's tendency to acquire third-party data. The first, seeking "legal guidance," describes "the improper capture of data" as follows:

> On occasion we encounter non-standard implementation of transmission control and Internet protocols within a network or at an ISP. Encountering non-standard implementation has led to *inadvertently capturing and processing data outside the Order or Consent*.[23]

The response, apparently written by a Bureau attorney, notes that "[s]uch unauthorized interceptions not only can violate a citizen's privacy but also can seriously 'contaminate' ongoing

---

[21] *Id.*

[22] E-mail message to Spike Bowman, dated April 5, 2000 (attached hereto as Exhibit B); *also available at* http://www.epic.org/privacy/carnivore/fisa.html. This document, as well as the other exhibits attached hereto, was not disclosed by the FBI until May 2002. *See, e.g.*, Dan Eggen, *"Carnivore" Glitches Blamed for FBI Woes; Problems With E-Mail Surveillance Program Led to Mishandling of al Qaeda Probe in 2000, Memo Says*, Washington Post, p. A7, May 29, 2002.

[23] Memorandum, untitled and undated (but apparently April 11, 2000) (attached hereto as Exhibit C); *also available at* http://www.epic.org/privacy/carnivore/questions.html (emphasis added).

investigations" and that such interceptions are "unlawful."[24] The author goes on to discuss "inadvertent, unauthorized interception[s]" that can occur when FBI technicians conduct tests of their packet-monitoring systems on the networks of ISPs:

> Somehow, when we test, we have to go out of our way to avoid tripping over innocent third party communications. I am not sure how we can proceed to test [Carnivore] without inadvertently intercepting the communications of others, but we really need to try.[25]

In the face of these facts — and with no reason to conclude that the documented instances of unlawful overcollection of packet communications would not markedly increase if CALEA's requirements were extended to new packet-mode technologies — the Commission would abdicate its responsibility to "protect the privacy and security of communications not authorized to be intercepted"[26] were it to expand CALEA's reach in the manner DOJ suggests.

Interestingly, the "legal guidance" on overcollection issues provided by FBI counsel recognizes that Congress has never considered the implications of the type of unauthorized interception of third-party communications detailed above. In discussing what are described as "interception accuracy" issues, the author notes that "historically" when authorized surveillance was conducted, "[t]ypical wire line service lent itself to reasonably easy segregation of a target's communications to the target line." The author then observes: "One possible exception being 'party-line' service, which by now is pretty rare. *Its [sic] unclear exactly what Congress would think about such party-line-related intercepts*."[27] Interception activity conducted on packet-mode voice networks, such as DOJ asks the Commission to facilitate, is the functional equivalent of "party-line-related intercepts" (although likely to implicate the privacy of far more non-target subscribers than would have been effected in the old-fashioned context). The Bureau thus concedes that Congress has not yet addressed the "interception accuracy" issues that are certain to arise from an expansion of surveillance capabilities in the packet-mode environment. As we

---

[24] Memorandum "RE: Internet/E-Mail Intercepts," dated April 12, 2000 (attached hereto as Exhibit D); *also available at* http://www.epic.org/privacy/carnivore/response.html.

[25] *Id.*

[26] 47 U.S.C. § 1006(b).

[27] Exhibit D (emphasis added).

have noted, it would be inappropriate for the Commission to consider such issues in the first instance.

III. DOJ Has Not Demonstrated Any Need for the Action It Requests

Finally, DOJ has not demonstrated that the existing CALEA regime is in any way inadequate to address its legitimate surveillance needs. Before the Commission opens a proceeding, especially on an "expedited" basis as DOJ requests, there should be a showing of necessity that goes beyond the anecdotal, unsubstantiated complaints that DOJ has put forward in its Joint Petition. While industry commenters will likely apprise the Commission of their "real-world" experiences in complying with law enforcement requests for assistance, we bring to the Commission's attention a prior DOJ assertion that appears to contradict much of the rationale that underlies the Joint Petition.

In its "field guidance" discussing the PATRIOT Act amendments relating to electronic surveillance, the Justice Department acknowledged that it is only in "infrequent cases" that ISPs are not able to provide law enforcement with requested information:

> *Generally*, when law enforcement serves a pen/trap order on a communication service provider that provides Internet access or other computing services to the public, *the provider itself should be able to collect the needed information and provide it to law enforcement.* In *certain rare cases*, however, the provider may be unable to carry out the court order, necessitating installation of a device (such as Etherpeek or the FBI's DCS1000) to collect the information.[28]

Thus, even in those "rare" and "infrequent" cases where service providers cannot fully comply with a court order, law enforcement has, through the use of its own technology, been able to obtain the information it seeks (and, as we have shown, sometimes more than that). The Joint Petition appears to be a proposed solution in search of a problem. DOJ has not met its burden of demonstrating the need for the proceeding it requests or the remedy it seeks.

CONCLUSION

In light of the clear legislative limitation of CALEA's scope; the presence of complex issues surrounding surveillance of packet-based networks that Congress has not yet addressed;

[28] Department of Justice, *Field Guidance on New Authorities That Relate to Computer Crime and Electronic Evidence Enacted in the USA Patriot Act of 2001*, *available at* http://www.usdoj.gov/criminal/cybercrime/PatriotAct.htm (emphasis added).

and DOJ's failure to show any need for the proceeding it requests, the Commission should decline DOJ's invitation to consider a radical expansion of CALEA's coverage. EPIC urges the Commission to deny the Joint Petition.

Respectfully Submitted,

David L. Sobel
Marc Rotenberg
Michael Trinh*

ELECTRONIC PRIVACY INFORMATION CENTER
1718 Connecticut Avenue, N.W.
Suite 200
Washington, DC 20009
(202) 483-1140

* IPIOP Law Clerk

April 12, 2004